Ken Amamori
4/15/2021

Q1. What are the IP address for utep.edu, engineering.utep.edu, and cs.utep.edu? Hint: nslookup

→

```
Kens-MBP:poking_around_assignment2 ken$ nslookup utep.edu
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   utep.edu
Address: 129.108.0.145
```

```
Kens-MBP:poking_around_assignment2 ken$ nslookup engineering.utep.edu
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
engineering.utep.edu    canonical name = engsrvweb00.utep.edu.
Name:   engsrvweb00.utep.edu
Address: 129.108.156.178
```

```
Kens-MBP:poking_around_assignment2 ken$ nslookup cs.utep.edu
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   cs.utep.edu
Address: 129.108.156.28
```

Q2. If a packet comes to me from 67.192.28.19 should I be suspicious? Why or why not? Hint: nslookup

→

Yes, because it is not a usual IP address, since mostly likely it starts with 3 digits numbers and this IP starting with 2 digits is ss[ocops. In addition, when running a command ‘nslookup 67.192.28.19’, the return is that server can’t find. Thus, a packet coming from 67.192.28.19 should not be trusted.

Ken Amamori
4/15/2021

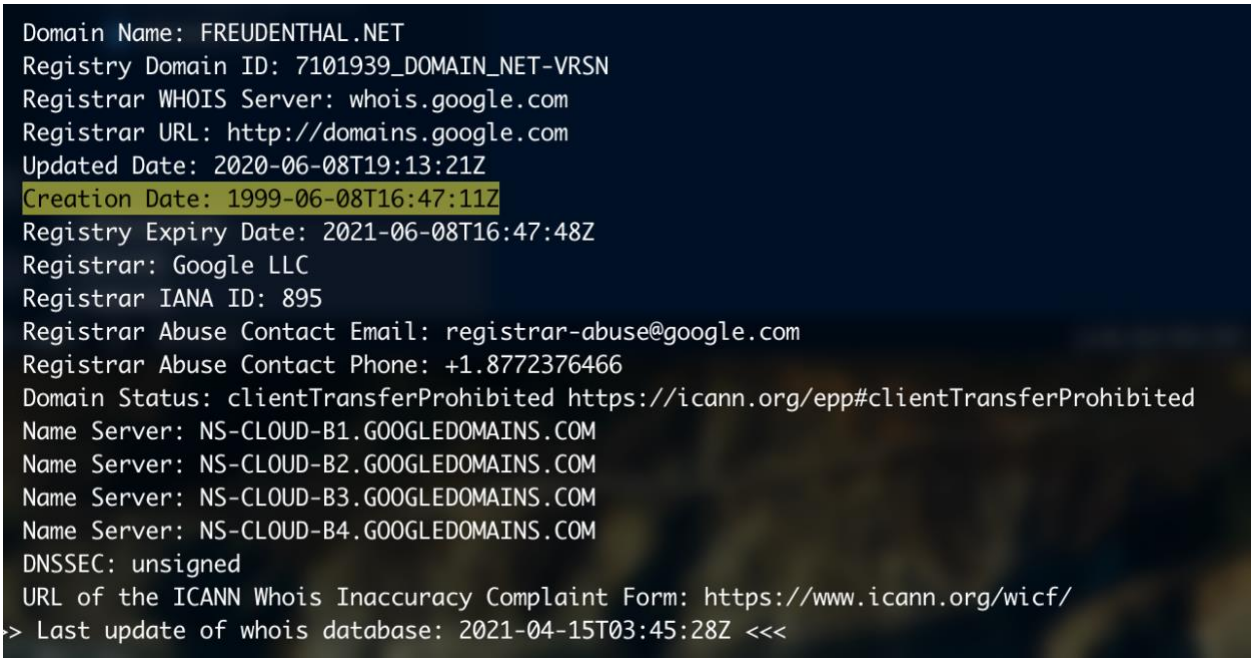
```
Kens-MBP:~ ken$ nslookup 67.192.28.19
Server:         192.168.1.254
Address:        192.168.1.254#53

** server can't find 19.28.192.67.in-addr.arpa: NXDOMAIN
```

Q3. Which domain is older, nigelward.com or freudenthal.net? Hint: whois
→
Command: *whois nigelward.com*

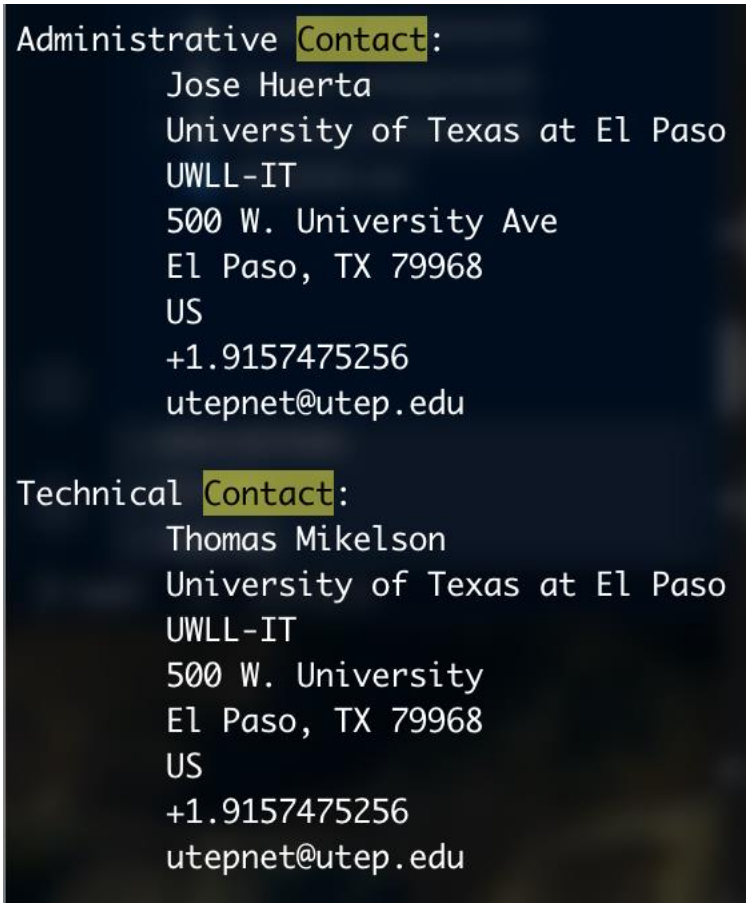
```
Domain Name: NIGELWARD.COM
Registry Domain ID: 81957414_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://www.tucows.com
Updated Date: 2018-10-08T19:45:42Z
Creation Date: 2002-01-04T00:40:38Z
Registry Expiry Date: 2024-01-04T00:40:38Z
Registrar: Tucows Domains Inc.
Registrar IANA ID: 69
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok https://icann.org/epp#ok
Name Server: DNS1.SERVERQUALITY.COM
Name Server: DNS2.SERVERQUALITY.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>> Last update of whois database: 2021-04-15T03:40:10Z <<<
```

Command: whois freudenthal.net



Comparing the date of creation between nigelward.com and fueudenthal.net, noted that freudenthal.net is older.

Q4. Who runs networking at UTEP? Hint: whois
→



Q5. How long can you confidently expect UTEP to remain at 129.108.0.145? Hint: nslookup -type=soa

→
Command: nslookup -type=soa utep.edu

Ken Amamori
4/15/2021

```
Kens-MBP:~ ken$ nslookup -type=soa utep.edu
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
utep.edu
        origin = dns4.utep.edu
        mail addr = utepnet.utep.edu
        serial = 799
        refresh = 3600
        retry = 1800
        expire = 86400
        minimum = 30400

Authoritative answers can be found from:
```

Q6. The argument to ping can be either a domain name or an IP address. For which of these does ping need to do a DNS lookup?

→

In both cases, since if a regular domain is given, it will return IP address. If IP address is given, retular domain will be returned. Thus, in eithercase, it will do “forward” dns lookup, and reverse dns lookup.